

UNITED STATES DISTRICT COURT

for the
Western District of WashingtonCERTIFIED TRUE COPY
ATTEST: WILLIAM M. MCCOOL
Clerk, U.S. District Court
Western District of WashingtonBy Sofia Patterson
Deputy ClerkIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)
The SUBJECT PREMISES, more fully described in
Attachment A

Case No. MJ21-101

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

The SUBJECT PREMISES, more fully described in Attachment A

located in the Western District of Washington, there is now concealed (identify the person or describe the property to be seized):

See Attachment B, incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C §§ 472 and 473	Uttering counterfeit obligations or securities and Dealing in counterfeit Obligations or securities

The application is based on these facts:

- ☒ See Affidavit of Special Agent Robert C. Patterson, continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☒ by reliable electronic means, or: ☐ telephonically recorded.

Applicant's signature

Robert C. Patterson, ICE Special Agent

Printed name and title

- ☐ The foregoing affidavit was sworn to before me and signed in my presence, or
- ☒ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: 02/22/2021

Judge's signature

City and state: Seattle, Washington

Brian A. Tsuchida, Chief United States Magistrate Judge

Printed name and title

AFFIDAVIT OF SA ROBERT C. PATTERSON

STATE OF WASHINGTON)
) ss
 COUNTY OF KING)

I, Robert C. Patterson, a Special Agent with United States Immigration and Customs Enforcement, Homeland Security Investigations, Seattle, Washington, having been duly sworn, state as follows:

AFFIANT BACKGROUND

1. I am a Special Agent (SA) with United States Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI) and have been so employed since March 2008. I have successfully completed the Federal Law Enforcement Training Center Criminal Investigator Training Program and the ICE-HSI Special Agent Training in Brunswick, Georgia. I have received additional training in complex commercial and trade fraud investigations at the United States Customs and Border Protection Advanced Training Facility in Harper's Ferry, West Virginia. I possess a bachelor's degree in Social Sciences from the University of Washington. As part of my duties as a Special Agent, I have participated in and led numerous investigations involving smuggling, drug trafficking, commercial fraud, intellectual property theft, money laundering, child exploitation, and work-site enforcement. Additionally, I have been involved in all aspects of criminal investigations including surveillance, undercover operations, and am authorized to serve and execute search and arrest warrants. Prior to my employment with ICE-HSI, I was on active duty in the United States Navy for two years and am presently a retired Naval Reservist.

2. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from other law enforcement agents and witnesses. This affidavit is intended to show that there is sufficient probable cause for the requested search warrant and does not purport to set forth all of my knowledge of this matter.

INTRODUCTION AND PURPOSE OF AFFIDAVIT

3. This affidavit is made in support of an anticipatory search warrant for the premises of [REDACTED] Marysville, Washington 98270 (the "SUBJECT PREMISES"), and any digital devices or electronic storage media located therein, for evidence of violations of Title 18, United States Code, Section 472 (Uttering counterfeit obligations or securities), and Section 473 (Dealing in counterfeit obligations). The SUBJECT PREMISES is more fully described in Attachment A to the search warrant. This warrant will not be executed until and unless the DHL package addressed to "Honda Civic [REDACTED] Marysville Washington 98270", described below in paragraph 5a-g is delivered to the SUBJECT PREMISES.

4. The items to be seized are evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 472 and 473. The items to be seized are listed in Attachment B to the search warrant.

SUMMARY OF PROBABLE CAUSE

5. On February 10, 2021, I received an email from Homeland Security Investigations Border Enforcement Security Taskforce officer located at the Los Angeles (California) International Mail Facility (HSI BEST IMF LAX). The email detailed a recent seizure by Customs and Border Protection (CBP) of a DHL international parcel inbound from Hong Kong. DHL is an international shipping firm. According to the officer:

a. The DHL parcel was intercepted by CBP on February 9, 2021

b. The DHL parcel was addressed to "Honda Civic [REDACTED] Marysville, Washington 98270" and had phone numbers "[REDACTED]" and printed below the address (hereafter the "SUBJECT PARCEL").

c. CBP Officers searched the SUBJECT PARCEL under their customs authority for overseas shipments. CBP Officers recovered \$485,300 in counterfeit \$100 Federal Reserve Notes inside the SUBJECT PARCEL. I sent photos taken of the parcel and notes to United States Secret Service (USSS), which determined based on the photos the notes were counterfeit. USSS keeps a database (called Counterfeit Tracking) of all reported counterfeit federal reserve notes. The database relies upon reports from

1 businesses, law enforcement, financial institutions and others. The federal reserve notes
 2 in the SUBJECT PARCEL all contain the same serial number. This serial number was
 3 queried by USSS in their database of known counterfeits and found a match. The
 4 photographs of the federal reserve notes in the SUBJECT PARCEL bearing serial
 5 number [REDACTED] along with other identifying marks, matched those of archived
 6 photos in the USSS database. The USSS reports there are more than 1,000 examples of
 7 this subject note being circulated in the United States. This counterfeit currency was first
 8 reported to the USSS on September 7, 2018 in the Portland, Oregon resident office.

9 d. The sender listed was "SZ ZHONGWU XINGHUA TECH CO
 10 LTD, QU WANRI, NANSHAN ZHI YUAN 101 XUEYUAN AVENUE, TAOYUAN
 11 STREET, NANSHAN DISTRICT, IF RTO, PLS RTN TO HKG FOR SHPR INST
 12 TSING YI, NO HONG KONG, HK."

13 e. The declaration section of the label stated "Date 2021-01-30" with
 14 "Description: Bar Prop 50PCS" and "Value: 50.00 USD" and "Weight: 3.500 KGS."

15 f. The Air Waybill number of the SUBJECT PARCEL is [REDACTED]

16 g. The SUBJECT PARCEL contained a Commercial Invoice number
 17 XS2205765 with a "Full Description of Goods" of "Bar Prop."

18 6. On February 10, 2021, I instructed HSI BEST IMF LAX to transfer custody
 19 of the SUBJECT PARCEL to HSI Seattle for further investigation. The SUBJECT
 20 PARCEL was received by HSI Seattle on February 18, 2021.

21 7. On February 10, 2021, I contacted United States Secret Service (USSS)
 22 Special Agent (SA) Jack Richards and provided details of the SUBJECT PARCEL. SA
 23 Richards instructed the USSS Investigative Support Division (ISD) to conduct law
 24 enforcement computer data base searches of the SUBJECT PREMISES. That search
 25 revealed the possible most recent occupants of the SUBJECT PREMISES as [REDACTED]

26 [REDACTED], and [REDACTED].

27 8. The USSS ISD conducted a Washington Department of Licensing search of
 28 [REDACTED] and [REDACTED]. That search revealed the same former address ([REDACTED]
 [REDACTED]) associated with both [REDACTED] and [REDACTED]
 Washington driver's licenses.

1 9. On February 18, 2021, ISD conducted a law enforcement computer
2 database search of telephone number [REDACTED] – the number printed below the
3 address on the SUBJECT PARCEL. No records were discovered related to this
4 telephone number.

5 10. On February 17, 2021, I conducted surveillance of the SUBJECT
6 PREMISES, [REDACTED] Marysville, Washington 98270. I observed a [REDACTED]
7 [REDACTED] parked in the parking stall labeled “1”. A
8 Washington Department of Licensing query revealed the vehicle is registered to [REDACTED]
9 [REDACTED] at the SUBJECT PREMISES.

10 11. On February 18, 2021, I contacted representatives from DHL to inquire
11 about the SUBJECT PARCEL. DHL informed me that, on or about February 12, 2021,
12 the consignee of the shipment [REDACTED] contacted DHL asking about the status of
13 the shipment, and if any duty, taxes, or fees are due. [REDACTED] provided DHL with
14 the phone number [REDACTED] and email address [REDACTED].

15 12. On February 18, 2021, United States Secret Service ISD conducted law
16 enforcement database queries of telephone number [REDACTED]. The telephone
17 number is a wireless telephone number assigned to [REDACTED].

18 13. On or about February 23, 2021, I and other agents intend to execute a
19 controlled delivery of the package to the SUBJECT PREMISES. Agents intend to
20 deliver the parcel to the SUBJECT PREMISES by knocking on the door of the apartment
21 and handing it to an occupant. If nobody answers the door, agents will leave the
22 SUBJECT PARCEL at the doorstep and maintain surveillance. Once the SUBJECT
23 PARCEL is retrieved and taken into the SUBJECT PREMISES, agents will execute the
24 search warrant of the SUBJECT PREMISES. Agents will search the SUBJECT
25 PREMISES for the SUBJECT PARCEL, and other evidence.

26 14. Based on my training and information that has become known to me
27 through communications with other law enforcement agents, I know the following:

28 a. Counterfeit United States currency is often stored in the suspect’s

1 residence.

2 b. Individuals who traffic in counterfeit currency often, in addition to
3 receiving and distributing counterfeit currency from other sources, also keep records
4 generated during the course of the scheme, including records related to the receipt and the
5 distribution of counterfeit currency, communications with other schemers, lists recording
6 names, addresses, and /or business associates, bank statements, telephone records, and
7 travel documents used in the furtherance of the counterfeit distribution scheme in their
8 homes or vehicles. Individuals who import and traffic in counterfeit currency often do so
9 to engage in other financial fraud schemes to launder the counterfeit currency into
10 legitimate monetary instruments, which further generates records often stored in their
11 homes or vehicles. All of these records may be stored on digital devices or electronic
12 storage media located in their homes or vehicles.

13 c. Individuals engaged in counterfeiting schemes will often use
14 electronic communications devices such as cellular telephones in order to communicate
15 with co-conspirators and to further their illegal activities. As a result, evidence of their
16 crimes can often be found in text messages, address books, call logs, photographs, emails,
17 text messaging or pictures messaging applications, videos, and other data that is stored on
18 cell phones, Blackberries, and other electronic communication devices;

19 d. The individuals use digital devices to place orders online for illicit
20 goods from foreign vendors or online sellers. They often communicate with the online
21 sellers and shippers via online communication platforms to include e-mail, instant
22 messaging services, text messaging services and encrypted communication platforms. As
23 a result, evidence of smuggling of counterfeit currency can be located in emails, text
24 messages, online accounts, and other data that is stored on cellphone, digital devices, and
25 electronic storage media.

26 **COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS**

27 15. As described above and in Attachment B, this application seeks permission
28 to search for evidence, fruits and/or instrumentalities that might be found at the
SUBJECT PREMISES, in whatever form they are found. One form in which the
evidence, fruits, and/or instrumentalities might be found is data stored on digital devices¹

¹ "Digital device" includes any device capable of processing and/or storing data in electronic form, including, but not limited to: central processing units, laptop, desktop, notebook or tablet computers, computer servers, peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media, related communications devices such as modems, routers and switches, and electronic/digital security devices, wireless communication devices such as mobile or cellular telephones and telephone paging devices,

such as computer hard drives or other electronic storage media.² Thus, the warrant applied for would authorize the seizure of digital devices or other electronic storage media or, potentially, the copying of electronically stored information from digital devices or other electronic storage media, all under Rule 41(e)(2)(B).

16. *Probable cause.* Based upon my review of the evidence gathered in this investigation, my review of data and records, information received from other agents and computer forensics examiners, and my training and experience, I submit that if a digital device or other electronic storage media is found at the SUBJECT PREMISES, there is probable cause to believe that evidence, fruits, and/or instrumentalities of the violations of Title 18, United States Code, Sections 472 and 473 will be stored on those digital devices or other electronic storage media. As set forth in Paragraph 14 above, I believe digital devices or other electronic storage media are being used in connection with the crimes under investigation. There is, therefore, probable cause to believe that evidence, fruits and/or instrumentalities of violations of Title 18, United States Code, Sections 472 and 473 exists and will be found on digital device or other electronic storage media at the SUBJECT PREMISES, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be preserved (and consequently also then recovered) for months or even years after they have been downloaded onto a storage medium, deleted, or accessed or viewed via the Internet. Electronic files downloaded to a digital device or other electronic storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a digital device or other electronic storage media, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

personal data assistants (“PDAs”), iPods/iPads, Blackberries, digital cameras, digital gaming devices, global positioning satellite devices (GPS), or portable media players.

² Electronic Storage media is any physical object upon which electronically stored information can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

1 b. Therefore, deleted files, or remnants of deleted files, may reside in
 2 free space or slack space—that is, in space on the digital device or other electronic
 3 storage medium that is not currently being used by an active file—for long periods of
 4 time before they are overwritten. In addition, a computer’s operating system may also
 5 keep a record of deleted data in a “swap” or “recovery” file.

6 c. Wholly apart from user-generated files, computer storage media—in
 7 particular, computers’ internal hard drives—contain electronic evidence of how a
 8 computer has been used, what it has been used for, and who has used it. To give a few
 9 examples, this forensic evidence can take the form of operating system configurations,
 10 artifacts from operating system or application operation; file system data structures, and
 11 virtual memory “swap” or paging files. Computer users typically do not erase or delete
 12 this evidence, because special software is typically required for that task. However, it is
 13 technically possible to delete this information.

14 d. Similarly, files that have been viewed via the Internet are sometimes
 15 automatically downloaded into a temporary Internet directory or “cache.”

16 17. *Forensic evidence.* As further described in Attachment B, this application
 17 seeks permission to locate not only computer files that might serve as direct evidence of
 18 the crimes described on the warrant, but also for forensic electronic evidence that
 19 establishes how digital devices or other electronic storage media were used, the purpose
 20 of their use, who used them, and when. There is probable cause to believe that this
 21 forensic electronic evidence will be on any digital devices or other electronic storage
 22 media located at the SUBJECT PREMISES because:

23 a. Stored data can provide evidence of a file that was once on the
 24 digital device or other electronic storage media but has since been deleted or edited, or of
 25 a deleted portion of a file (such as a paragraph that has been deleted from a word
 26 processing file). Virtual memory paging systems can leave traces of information on the
 27 digital device or other electronic storage media that show what tasks and processes were
 28 recently active. Web browsers, e-mail programs, and chat programs store configuration
 information that can reveal information such as online nicknames and passwords.
 Operating systems can record additional information, such as the history of connections
 to other computers, the attachment of peripherals, the attachment of USB flash storage
 devices or other external storage media, and the times the digital device or other
 electronic storage media was in use. Computer file systems can record information about
 the dates files were created and the sequence in which they were created. _____

1 b. As explained herein, information stored within a computer and other
2 electronic storage media may provide crucial evidence of the “who, what, why, when,
3 where, and how” of the criminal conduct under investigation, thus enabling the United
4 States to establish and prove each element or alternatively, to exclude the innocent from
5 further suspicion. In my training and experience, information stored within a computer
6 or storage media (e.g., registry information, communications, images and movies,
7 transactional information, records of session times and durations, internet history, and
8 anti-virus, spyware, and malware detection programs) can indicate who has used or
9 controlled the computer or storage media. This “user attribution” evidence is analogous
10 to the search for “indicia of occupancy” while executing a search warrant at a residence.
11 The existence or absence of anti-virus, spyware, and malware detection programs may
12 indicate whether the computer was remotely accessed, thus inculcating or exculpating the
13 computer owner and/or others with direct physical access to the computer. Further,
14 computer and storage media activity can indicate how and when the computer or storage
15 media was accessed or used. For example, as described herein, computers typically
16 contain information that log: computer user account session times and durations,
17 computer activity associated with user accounts, electronic storage media that connected
18 with the computer, and the IP addresses through which the computer accessed networks
19 and the internet. Such information allows investigators to understand the chronological
20 context of computer or electronic storage media access, use, and events relating to the
21 crime under investigation. Additionally, some information stored within a computer or
22 electronic storage media may provide crucial evidence relating to the physical location of
23 other evidence and the suspect. For example, images stored on a computer may both
24 show a particular location and have geolocation information incorporated into its file
25 data. Such file data typically also contains information indicating when the file or image
26 was created. The existence of such image files, along with external device connection
27 logs, may also indicate the presence of additional electronic storage media (e.g., a digital
28 camera or cellular phone with an incorporated camera). The geographic and timeline
information described herein may either inculcate or exculpate the computer user. Last,
information stored within a computer may provide relevant insight into the computer
user’s state of mind as it relates to the offense under investigation. For example,
information within the computer may indicate the owner’s motive and intent to commit a
crime (e.g., internet searches indicating criminal planning), or consciousness of guilt
(e.g., running a “wiping” program to destroy evidence on the computer or password
protecting/encrypting such evidence in an effort to conceal it from law enforcement).

25 c. A person with appropriate familiarity with how a digital device or
26 other electronic storage media works can, after examining this forensic evidence in its
27 proper context, draw conclusions about how the digital device or other electronic storage
28 media were used, the purpose of their use, who used them, and when. _____

1 d. The process of identifying the exact files, blocks, registry entries,
2 logs, or other forms of forensic evidence on a digital device or other electronic storage
3 media that are necessary to draw an accurate conclusion is a dynamic process. While it is
4 possible to specify in advance the records to be sought, digital evidence is not always
5 data that can be merely reviewed by a review team and passed along to investigators.
6 Whether data stored on a computer is evidence may depend on other information stored
7 on the computer and the application of knowledge about how a computer behaves.
8 Therefore, contextual information necessary to understand other evidence also falls
9 within the scope of the warrant.

10 e. Further, in finding evidence of how a digital device or other
11 electronic storage media was used, the purpose of its use, who used it, and when,
12 sometimes it is necessary to establish that a particular thing is not present. For example,
13 the presence or absence of counter-forensic programs or anti-virus programs (and
14 associated data) may be relevant to establishing the user's intent.

15 18. As set forth in Paragraph 14, above, there is probable cause to believe that
16 the digital devices are instrumentalities of the crimes because they were used to facilitate
17 the receipt or intended distribution of the counterfeit currency, communicate with other
18 schemers, or in other ways.

19 19. There have been no prior efforts to obtain electronically stored evidence
20 from the targets, as this is a covert investigation. I believe, based upon the nature of the
21 investigation and the information I have received, that if the targets become aware of the
22 investigation in advance of the execution of a search warrant, they may attempt to destroy
23 any potential evidence, whether digital or non-digital, thereby hindering law enforcement
24 agents from the furtherance of the criminal investigation.

25 20. I know based on my training and experience that digital information can be
26 very fragile and easily destroyed. Digital information can also be easily encrypted or
27 obfuscated such that review of the evidence would be extremely difficult, and in some
28 cases impossible. If an encrypted computer is either powered off or if the user has not
entered the encryption password and logged onto the computer, it is likely that any
information contained on the computer will be impossible to decipher. If the computer is
powered on, however, and the user is already logged onto the computer, there is a much

1 greater chance that the digital information can be extracted from the computer. This is
2 because when the computer is on and in use, the password has already been entered and
3 the data on the computer is accessible. However, giving the owner of the computer time
4 to activate a digital security measure, pull the power cord from the computer, or even log
5 off of the computer could result in a loss of digital information that could otherwise have
6 been extracted from the computer.

7 21. *Necessity of seizing or copying entire computers or storage media.* In most
8 cases, a thorough search of premises for information that might be stored on digital
9 devices or other electronic storage media often requires the seizure of the physical items
10 and later off-site review consistent with the warrant. In lieu of removing all of these
11 items from the premises, it is sometimes possible to make an image copy of the data on
12 the digital devices or other electronic storage media, onsite. Generally speaking, imaging
13 is the taking of a complete electronic picture of the device's data, including all hidden
14 sectors and deleted files. Either seizure or imaging is often necessary to ensure the
15 accuracy and completeness of data recorded on the item, and to prevent the loss of the
16 data either from accidental or intentional destruction. This is true because of the
17 following:

18 a. The time required for an examination. As noted above, not all
19 evidence takes the form of documents and files that can be easily viewed on site.
20 Analyzing evidence of how a computer has been used, what it has been used for, and who
21 has used it requires considerable time, and taking that much time on premises could be
22 unreasonable. As explained above, because the warrant calls for forensic electronic
23 evidence, it is exceedingly likely that it will be necessary to thoroughly examine the
24 respective digital device and/or electronic storage media to obtain evidence. Computer
25 hard drives, digital devices and electronic storage media can store a large volume of
26 information. Reviewing that information for things described in the warrant can take
27 weeks or months, depending on the volume of data stored, and would be impractical and
28 invasive to attempt on-site.

26 b. Technical requirements. Digital devices or other electronic storage
27 media can be configured in several different ways, featuring a variety of different
28 operating systems, application software, and configurations. Therefore, searching them
sometimes requires tools or knowledge that might not be present on the search site. The

1 vast array of computer hardware and software available makes it difficult to know before
 2 a search what tools or knowledge will be required to analyze the system and its data on
 3 the premises. However, taking the items off-site and reviewing them in a controlled
 environment will allow examination with the proper tools and knowledge.

4 c. Variety of forms of electronic media. Records sought under this
 5 warrant could be stored in a variety of electronic storage media formats and on a variety
 6 of digital devices that may require off-site reviewing with specialized forensic tools.

7 22. Based on the foregoing, and consistent with Rule 41(e)(2)(B) of the Federal
 8 Rules of Criminal Procedure, the warrant I am applying for will permit seizing, imaging,
 9 or otherwise copying digital devices or other electronic storage media that reasonably
 10 appear capable of containing some or all of the data or items that fall within the scope of
 11 Attachment B to this Affidavit, and will specifically authorize a later review of the media
 12 or information consistent with the warrant. [REDACTED]

13 23. Consistent with the above, I hereby request the Court's permission to seize
 14 and/or obtain a forensic image of digital devices or other electronic storage media that
 15 reasonably appear capable of containing data or items that fall within the scope of
 16 Attachment B to this Affidavit, and to conduct off-site searches of the digital devices or
 17 other electronic storage media and/or forensic images, using the following procedures:

18 24. *Processing the Search Sites and Securing the Data*

19 a. Upon securing the physical search site, the search team will conduct
 20 an initial review of any digital devices or other electronic storage media located at the
 21 subject premises described in Attachment A that are capable of containing data or items
 22 that fall within the scope of Attachment B to this Affidavit, to determine if it is possible
 to secure the data contained on these devices onsite in a reasonable amount of time and
 without jeopardizing the ability to accurately preserve the data.

23 b. In order to examine the electronically stored information ("ESI") in
 24 a forensically sound manner, law enforcement personnel with appropriate expertise will
 25 attempt to produce a complete forensic image, if possible and appropriate, of any digital

1 device or other electronic storage media that is capable of containing data or items that
2 fall within the scope of Attachment B to this Affidavit.³

3 c. A forensic image may be created of either a physical drive or a
4 logical drive. A physical drive is the actual physical hard drive that may be found in a
5 typical computer. When law enforcement creates a forensic image of a physical drive,
6 the image will contain every bit and byte on the physical drive. A logical drive, also
7 known as a partition, is a dedicated area on a physical drive that may have a drive letter
8 assigned (for example the c: and d: drives on a computer that actually contains only one
9 physical hard drive). Therefore, creating an image of a logical drive does not include
10 every bit and byte on the physical drive. Law enforcement will only create an image of
11 physical or logical drives physically present on or within the subject device. Creating an
12 image of the devices located at the search locations described in Attachment A will not
13 result in access to any data physically located elsewhere. However, digital devices or
14 other electronic storage media at the search locations described in Attachment A that
15 have previously connected to devices at other locations may contain data from those
16 other locations. _____

17 d. If based on their training and experience, and the resources available
18 to them at the search site, the search team determines it is not practical to make an on-site
19 image within a reasonable amount of time and without jeopardizing the ability to
20 accurately preserve the data, then the digital devices or other electronic storage media
21 will be seized and transported to an appropriate law enforcement laboratory to be
22 forensically imaged and reviewed. _____

23 25. *Searching the Forensic Images*

24 a. Searching the forensic images for the items described in Attachment
25 B may require a range of data analysis techniques. In some cases, it is possible for agents
26 and analysts to conduct carefully targeted searches that can locate evidence without
27 requiring a time-consuming manual search through unrelated materials that may be
28 commingled with criminal evidence. In other cases, however, such techniques may not
yield the evidence described in the warrant, and law enforcement may need to conduct


³ The purpose of using specially trained computer forensic examiners to conduct the imaging of digital devices or other electronic storage media is to ensure the integrity of the evidence and to follow proper, forensically sound, scientific procedures. When the investigative agent is a trained computer forensic examiner, it is not always necessary to separate these duties. Computer forensic examiners often work closely with investigative personnel to assist investigators in their search for digital evidence. Computer forensic examiners are needed because they generally have technological expertise that investigative agents do not possess. Computer forensic examiners, however, often lack the factual and investigative expertise that an investigative agent may possess on any given case. Therefore, it is often important that computer forensic examiners and investigative personnel work closely together.

1 more extensive searches to locate evidence that falls within the scope of the warrant. The
2 search techniques that will be used will be only those methodologies, techniques and
3 protocols as may reasonably be expected to find, identify, segregate and/or duplicate the
4 items authorized to be seized pursuant to Attachment B to this affidavit. Those
5 techniques, however, may necessarily expose many or all parts of a hard drive to human
6 inspection in order to determine whether it contains evidence described by the warrant.


7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

CONCLUSION

26. Based on the foregoing, I request that the Court issue the proposed warrant and seal all material in support of this application. This is a covert investigation, and premature disclosure of the warrant, affidavit, or other material may alert the targets and result in the destruction of evidence, flight of the suspects, or change in behavior by the suspects.


ROBERT C. PATTERSON, Affiant
Special Agent, DHS-ICE

The above-named officer provided a sworn statement attesting to the truth of the contents of the foregoing affidavit this 22nd day of February, 2021.


BRIAN A. TSUCHIDA
Chief United States Magistrate Judge

ATTACHMENT B
Items to be Seized

The following records, documents, files, or materials, in whatever form, including handmade or mechanical form (such as printed, written, handwritten, or typed); photocopies or other photographic form; and electrical, electronic, and magnetic form (such as tapes, cassettes, hard disks, floppy disks, diskettes, compact discs, CD-ROMs, DVDs, optical discs, Zip cartridges, printer buffers, smart cards, or electronic notebooks, or any other electronic storage medium) that constitute evidence, instrumentalities, or fruits of violations of Title 18, United States Code, Sections 472 and 473:

1. Counterfeit currency;
2. Records of the distribution, purchase, or importation of counterfeit currency, including but not limited to, inventories, ledgers, journals, financial statements, check registers, notes, bills of lading, commercial invoices, shipping labels and parcels, and correspondence;
3. Lists or other writings recording the names, addresses, or telephone numbers of customers and/or business associates, including but not limited to, telephone books, address books, calendars, or other items or lists reflecting names, addresses, or telephone numbers of customers and/or business associates;
4. Bank statements, records, and records of wire transfers;
5. Telephone toll records and bills;
6. Travel documents, including but not limited to, passports, travel receipts, airline tickets, and charge receipts;
7. Items of personal property and documents tending to establish the identity of the person(s) in control of the premises, including rent receipts, utility company receipts, telephone bills, canceled checks, bank statements, and canceled mail envelopes;
8. Currency, in any form, constituting the proceeds of the counterfeit distribution scheme;

9. Digital devices¹ or other electronic storage media² and/or their components, which include:
 - a. Any digital device or other electronic storage media capable of being used to commit, further, or store evidence of the offenses listed above;
 - b. Any digital devices or other electronic storage media used to facilitate the transmission, creation, display, encoding or storage of data, including word processing equipment, modems, docking stations, monitors, cameras, printers, plotters, encryption devices, and optical scanners;
 - c. Any magnetic, electronic or optical storage device capable of storing data, such as floppy disks, hard disks, tapes, CD-ROMs, CD-R, CD-RWs, DVDs, optical disks, printer or memory buffers, smart cards, PC cards, memory calculators, electronic dialers, electronic notebooks, and personal digital assistants;
 - d. Any documentation, operating logs and reference manuals regarding the operation of the digital device or other electronic storage media or software;
 - e. Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices, or data to be searched;
 - f. Any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the computer equipment, storage devices or data; and
 - g. Any passwords, password files, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data.
10. For any digital device or other electronic storage media upon which electronically stored information that is called for by this warrant may be

¹ "Digital device" includes any device capable of processing and/or storing data in electronic form, including, but not limited to: central processing units, laptop, desktop, notebook or tablet computers, computer servers, peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media, related communications devices such as modems, routers and switches, and electronic/digital security devices, wireless communication devices such as mobile or cellular telephones and telephone paging devices, personal data assistants ("PDAs"), iPods/iPads, Blackberries, digital cameras, digital gaming devices, global positioning satellite devices (GPS), or portable media players.

² Electronic Storage media is any physical object upon which electronically stored information can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

1 contained, or that may contain things otherwise called for by this warrant,
2 and in addition to the items set forth above:

- 3 a. evidence of who used, owned, or controlled the digital device or
4 other electronic storage media at the time the things described in this
5 warrant were created, edited, or deleted, such as logs, registry
6 entries, configuration files, saved usernames and passwords,
7 documents, browsing history, user profiles, email, email contacts,
8 "chat," instant messaging logs, photographs, and correspondence;
9
10 b. evidence of software that would allow others to control the digital
11 device or other electronic storage media, such as viruses, Trojan
12 horses, and other forms of malicious software, as well as evidence
13 of the presence or absence of security software designed to detect
14 malicious software;
15
16 c. evidence of the lack of such malicious software;
17
18 d. evidence of the attachment to the digital device of other storage
19 devices or similar containers for electronic evidence;
20
21 e. evidence of counter-forensic programs (and associated data) that are
22 designed to eliminate data from the digital device or other electronic
23 storage media;
24
25 f. evidence of the times the digital device or other electronic storage
26 media was used;
27
28 g. passwords, encryption keys, and other access devices that may be
necessary to access the digital device or other electronic storage
media;
h. documentation and manuals that may be necessary to access the
digital device or other electronic storage media or to conduct a
forensic examination of the digital device or other electronic storage
media;
i. contextual information necessary to understand the evidence
described in this attachment.

11. Cellular phones may be searched only for the following items:
- i. Assigned number and identifying telephone serial number (ESN, MIN, IMSI, or IMEI);
 - ii. Stored list of recent received calls;
 - iii. Stored list of recent sent/dialed calls;
 - iv. Stored contact information;
 - v. Stored photographs of related to crimes under investigation and/or co-conspirators; and
 - vi. Stored text messages related to the crimes under investigation.

THE SEIZURE OF DIGITAL DEVICES OR OTHER ELECTRONIC STORAGE MEDIA AND/OR THEIR COMPONENTS AS SET FORTH HEREIN IS SPECIFICALLY AUTHORIZED BY THIS SEARCH WARRANT, NOT ONLY TO THE EXTENT THAT SUCH DIGITAL DEVICES OR OTHER ELECTRONIC STORAGE MEDIA CONSTITUTE INSTRUMENTALITIES OF THE CRIMINAL ACTIVITY DESCRIBED ABOVE, BUT ALSO FOR THE PURPOSE OF THE CONDUCTING OFF-SITE EXAMINATIONS OF THEIR CONTENTS FOR EVIDENCE, INSTRUMENTALITIES, OR FRUITS OF THE AFOREMENTIONED CRIMES.